

**GAO**

Report to the Chairman and Ranking  
Minority Member, Committee on  
Government Reform, House of  
Representatives

---

February 2003

# FILE-SHARING PROGRAMS

## Peer-to-Peer Networks Provide Ready Access to Child Pornography





Highlights of [GAO-03-351](#), a report to the Chairman and Ranking Minority Member, Committee on Government Reform, House of Representatives

## Why GAO Did This Study

The availability of child pornography has dramatically increased in recent years as it has migrated from printed material to the World Wide Web, becoming accessible through Web sites, chat rooms, newsgroups, and now the increasingly popular peer-to-peer file-sharing programs. These programs enable direct communication between users, allowing users to access each other's files and share digital music, images, and video.

GAO was requested to determine the ease of access to child pornography on peer-to-peer networks; the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography; and the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

Because child pornography cannot be accessed legally other than by law enforcement agencies, GAO worked with the Customs Cyber-Smuggling Center in performing searches: Customs downloaded and analyzed image files, and GAO performed analyses based on keywords and file names only.

In commenting on a draft of this report, the Department of Justice agreed with the report's findings and provided additional information.

[www.gao.gov/cgi-bin/getrpt?GAO-03-351](http://www.gao.gov/cgi-bin/getrpt?GAO-03-351).

To view the full report, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or [koontzl@gao.gov](mailto:koontzl@gao.gov).

## FILE-SHARING PROGRAMS

### Peer-to-Peer Networks Provide Ready Access to Child Pornography

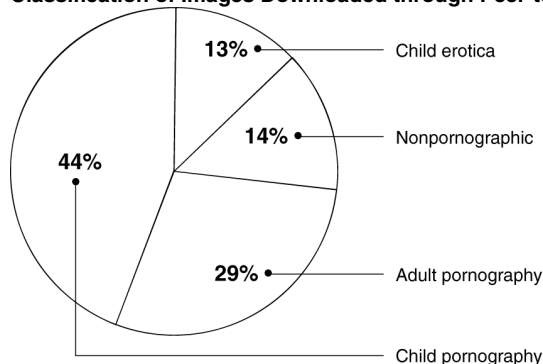
#### What GAO Found

Child pornography is easily found and downloaded from peer-to-peer networks. In one search using 12 keywords known to be associated with child pornography on the Internet, GAO identified 1,286 titles and file names, determining that 543 (about 42 percent) were associated with child pornography images. Of the remaining, 34 percent were classified as adult pornography and 24 percent as nonpornographic. In another search using three keywords, a Customs analyst downloaded 341 images, of which 149 (about 44 percent) contained child pornography (see the figure below). These results are in accord with increased reports of child pornography on peer-to-peer networks; since it began tracking these in 2001, the National Center for Missing and Exploited Children has seen a fourfold increase—from 156 in 2001 to 757 in 2002. Although the numbers are as yet small by comparison to those for other sources (26,759 reports of child pornography on Web sites in 2002), the increase is significant.

Juvenile users of peer-to-peer networks are at significant risk of inadvertent exposure to pornography, including child pornography. Searches on innocuous keywords likely to be used by juveniles (such as names of cartoon characters or celebrities) produced a high proportion of pornographic images: in our searches, the retrieved images included adult pornography (34 percent), cartoon pornography (14 percent), child erotica (7 percent), and child pornography (1 percent).

While federal law enforcement agencies—including the FBI, Justice's Child Exploitation and Obscenity Section, and Customs—are devoting resources to combating child exploitation and child pornography in general, these agencies do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet. Therefore, GAO was unable to quantify the resources devoted to investigating cases on peer-to-peer networks. According to law enforcement officials, however, as tips concerning child pornography on peer-to-peer networks escalate, law enforcement resources are increasingly being focused on this area.

Classification of Images Downloaded through Peer-to-Peer File-Sharing Program



Source: Customs CyberSmuggling Center.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Results in Brief	2
	Background	3
	Peer-to-Peer Applications Provide Easy Access to Child Pornography	11
	Juvenile Users of Peer-to-Peer Applications May Be Inadvertently Exposed to Pornography	14
	Federal Law Enforcement Agencies Are Beginning to Focus Resources on Child Pornography on Peer-to-Peer Networks	15
	Conclusions	17
	Agency Comments and Our Evaluation	17
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	<b>19</b>
<b>Appendix II</b>	<b>Description of File Sharing and Peer-to-Peer Networks</b>	<b>21</b>
<b>Appendix III</b>	<b>Comments from the Department of Justice</b>	<b>26</b>
<b>Glossary</b>		<b>29</b>
<b>Tables</b>		
	Table 1: Internet Technologies Providing Access to Child Pornography	7
	Table 2: Organizations and Agencies Involved with Peer-to-Peer Child Pornography Efforts	9
	Table 3: NCMEC CyberTipline Referrals to Law Enforcement Agencies, Fiscal Years 1998–2002	14
<b>Figures</b>		
	Figure 1: Classification of 1,286 Titles and File Names of Images Identified in KaZaA Search	12
	Figure 2: Classification of 341 Images Downloaded through KaZaA	13

---

Figure 3: Classification of 177 Images of a Popular Singer, Child Actors, and a Cartoon Character Downloaded through KaZaA	15
Figure 4: Peer-to-Peer Models	22
Figure 5: Topology of a Gnutella Network	25

---

### Abbreviations

CEOS	Child Exploitation and Obscenity Section
FBI	Federal Bureau of Investigation
IRC	Internet Relay Chat
MP3	Moving Pictures Experts Group (MPEG) MPEG-1 Audio Layer-3
NCMEC	National Center for Missing and Exploited Children
NCVIP	National Child Victim Identification Program
NRC	National Research Council
P2P	peer to peer
URL	Uniform Resource Locator
VNS	virtual name space

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.



G A O

Accountability \* Integrity \* Reliability

United States General Accounting Office  
Washington, DC 20548

---

February 20, 2003

The Honorable Tom Davis  
Chairman  
The Honorable Henry A. Waxman  
Ranking Minority Member  
Committee on Government Reform  
House of Representatives

The availability of child pornography has dramatically increased in recent years as it has migrated from magazines, photographs, and videos to the World Wide Web. The Internet's wide range of information search and retrieval technologies, which make it possible to quickly find a vast array of information, also make it easy to access, disseminate, and trade pornographic images and videos, including child pornography. Increasingly, child pornography is accessible through Web sites, chat rooms, newsgroups, and the increasingly popular peer-to-peer technology, which allows direct communication between computer users, so that they can access and share each other's files (including images, video, and software).

As requested, our objectives were to determine (1) the ease of access to child pornography on peer-to-peer networks; (2) the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography; and (3) the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

To address the first two objectives, we were assisted by the U.S. Customs CyberSmuggling Center in using a peer-to-peer application to search for image files matching keywords that were intended to identify pornography and child pornography images or that might accidentally identify pornographic images. The resulting files were downloaded, saved, analyzed, and classified by a U.S. Customs CyberSmuggling agent.<sup>1</sup> To determine what federal law enforcement resources are allocated to combating child pornography on peer-to-peer networks, we analyzed

---

<sup>1</sup>Because child pornography cannot be accessed legally other than by law enforcement agencies, we relied on Customs to download and analyze image files. We performed analyses based on titles and file names only.

---

resource allocation data at the Federal Bureau of Investigation and the Child Exploitation and Obscenity Section within the Department of Justice, and at the U.S. Customs Service and U.S. Secret Service within the Department of the Treasury. We also received documentation about what resources were being allocated to combat child pornography from the National Center for Missing and Exploited Children, a federally funded nonprofit organization that serves as a national resource center for information related to crimes against children.

Appendix I contains a more detailed discussion of our objectives, scope, and methodology. Appendix II provides more information on the characteristics and use of peer-to-peer file-sharing programs.

---

## Results in Brief

Child pornography is easily accessed and downloaded from peer-to-peer networks. Using KaZaA, a popular peer-to-peer file-sharing program, we used 12 keywords known to be associated with child pornography on the Internet to search for child pornography image files. We identified 1,286 items, each with a title and file name, determining that 543 (about 42 percent) were associated with child pornography images. Of the remaining, 34 percent were classified as adult pornography and 24 percent as nonpornographic. In another search using three keywords, the Customs CyberSmuggling Center also used KaZaA to search for and download child pornography image files.<sup>2</sup> This search identified 341 image files, of which 149 (about 44 percent) were classified as child pornography.<sup>3</sup> The remaining images were classified as child erotica<sup>4</sup> (13 percent), adult pornography (29 percent), or other (nonpornographic) images (14 percent). These results are consistent with observations of the National Center for Missing and Exploited Children, which has stated that peer-to-peer technology is increasingly popular for the dissemination of child pornography. Although peer-to-peer networks are currently not the most prominent source for child pornography, law enforcement agencies have noted a significant increase in their use for this purpose. Since 2001, when the center began to track peer-to-peer child pornography, peer-to-peer

---

<sup>2</sup>Other popular peer-to-peer applications include Gnutella, BearShare, LimeWire, and Morpheus.

<sup>3</sup>Customs downloaded and analyzed image files for us because child pornography can be legally accessed only by law enforcement agencies.

<sup>4</sup>Erotic images of children that do not depict sexually explicit conduct.

---

reports have increased more than fourfold—from 156 in 2001 to 757 in 2002.

When searching and downloading images on peer-to-peer networks, juvenile users face a significant risk of inadvertent exposure to pornography, including child pornography. Searches on innocuous keywords likely to be used by juveniles produce images of which a high proportion are pornographic: in our searches, the retrieved images included adult pornography (34 percent), cartoon pornography<sup>5</sup> (14 percent), child erotica (7 percent), and child pornography (1 percent).

We were unable to determine the precise extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks. While several law enforcement agencies—including the Federal Bureau of Investigation, Justice’s Child Exploitation and Obscenity Section, and Customs—devote resources to combating child exploitation and child pornography in general, they do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet. Therefore, we were unable to quantify the resources devoted to investigations of peer-to-peer networking. Law enforcement officials told us, however, that as they receive larger numbers of tips concerning child pornography on peer-to-peer networks, they are focusing more law enforcement resources in this area.

In commenting on a draft of this report, the Department of Justice agreed with the report’s findings and provided some additional information; Justice’s comments are reprinted in appendix III. We also received technical comments from the U.S. Secret Service and the U.S. Customs Service. Their comments have been incorporated in the report as appropriate.

---

## Background

Federal statutes provide for civil and criminal penalties for the production, advertising, possession, receipt, distribution, and sale of child pornography.<sup>6</sup> Of particular relevance to this report, the child pornography statutes prohibit the use of any means of interstate or foreign commerce (which will typically include the use of an interactive computer service) to sell, advertise, distribute, receive, or possess child pornography.

---

<sup>5</sup>Images of cartoon characters depicting sexually explicit conduct.

<sup>6</sup>See chapter 110 of Title 18, U.S. Code.

---

Additionally, federal obscenity statutes prohibit the use of any means of interstate or foreign commerce or an interactive computer service to import, transport, or distribute obscene material or to transfer obscene material to persons under the age of 16.<sup>7</sup>

Child pornography is defined by statute as the visual depiction of a minor—a person under 18 years of age—engaged in sexually explicit conduct.<sup>8</sup> By contrast, for material to be defined as obscene depends on whether an average person, applying contemporary community standards, would interpret the work—including images—to appeal to the prurient interest and to be patently offensive, and whether a reasonable person would find the material lacks serious literary, artistic, political, or scientific value.<sup>9</sup>

In addition to making it a crime to transport, receive, sell, distribute, advertise, or possess child pornography in interstate or foreign commerce, federal child pornography statutes prohibit, among other things, the use of a minor in producing pornography, and they provide for criminal and civil forfeiture of real and personal property used in making child pornography and of the profits of child pornography.<sup>10</sup> Child pornography, which is intrinsically related to the sexual abuse of children, is unprotected by the First Amendment.<sup>11</sup> Nor does the First Amendment protect the production, distribution, or transfer of obscene material.<sup>12</sup>

---

<sup>7</sup>See chapter 71 of Title 18, U.S. Code.

<sup>8</sup>See 18 U.S.C. § 2256(8).

<sup>9</sup>See *Miller v. California*, 413 U.S. 15 (1973). In *Miller*, the Supreme Court created a three-part test to determine whether a work is obscene. The *Miller* test, as interpreted by subsequent Supreme Court jurisprudence, asks (a) whether an average person applying contemporary community standards would find that the material, taken as a whole, appeals to the prurient interest; (b) whether an average person applying contemporary community standards would find that the material depicts proscribed behavior in a patently offensive manner; and (c) whether a reasonable person would find that the material, taken as a whole, lacks serious literary, artistic, political, or scientific value. As the *Miller* test is unrelated to child pornography, it does not account for the government's compelling interest in protecting children from sexual exploitation.

<sup>10</sup>See chapter 110, Title 18, U.S. Code.

<sup>11</sup>See *New York v. Ferber*, 458 U.S. 747 (1982).

<sup>12</sup>See *Roth v. United States*, 354 U.S. 476 (1957). In contrast, the private possession of obscenity in one's home is protected by the First Amendment. See *Stanley v. Georgia*, 394 U.S. 557 (1969).



---

In enacting the Child Pornography Prevention Act of 1996,<sup>13</sup> Congress sought to expand the federal prohibition against child pornography from images that involve actual children to sexually explicit images that only appear to depict minors but were produced without using any real children. The act defines child pornography as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture” that “is, or appears to be, of a minor engaging in sexually explicit conduct” or is “advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.” Last year, the Supreme Court struck down this legislative attempt to ban “virtual” child pornography<sup>14</sup> in *Ashcroft v. The Free Speech Coalition*, ruling that the expansion of the act to material that did not involve and thus harm actual children in its creation is an unconstitutional violation of free speech rights. According to government officials, this ruling may increase the difficulty faced by law enforcement agencies in prosecuting those who produce and possess child pornography. Since the government must establish that the digital images of children engaged in sexual acts are those of real children, it may be difficult to prosecute cases in which the defendants claim that the images in question are of “virtual” children.

---

<sup>13</sup>Section 121, P.L. 104-208, 110 Stat. 3009-26.

<sup>14</sup>According to the Justice Department, rapidly advancing technology has raised the possibility of creating images of child pornography without the use of a real child (“virtual” child pornography). Totally virtual creations would be both time intensive and, for now, prohibitively costly to produce. However, the technology has led to a ready defense (the “virtual” porn defense) against prosecution under laws that are limited to sexually explicit depictions of *actual* minors. Because the technology does exist today to alter images in a manner that disguises the identity of the real child or makes the image seem computer-generated, it encourages producers and distributors of child pornography to alter depictions of actual children in slight ways to make them not only unidentifiable, but also appear as if they were virtual creations—and thereby attempt to defeat prosecution. In contrast to the weighty task of creating an entire image out of whole cloth, it is not difficult or expensive to use readily available technology to disguise depictions of real children to make them unidentifiable or to make them appear computer generated.

---

## The Internet Has Emerged as the Principal Tool for Exchanging Child Pornography

Historically, pornography, including child pornography, tended to be found mainly in photographs, magazines, and videos.<sup>15</sup> The arrival and the rapid expansion of the Internet and its technologies, the increased availability of broadband Internet services, advances in digital imaging technologies, and the availability of powerful digital graphic programs have brought about major changes in both the volume and the nature of available child pornography. The proliferation of child pornography on the Internet is prompting wide concern. According to a recent survey, over 90 percent of Americans say they are concerned about child pornography on the Internet, and 50 percent of Americans cite child pornography as the single most heinous crime that takes place on line.<sup>16</sup>

According to experts, pornographers have traditionally exploited—and sometimes pioneered—emerging communication technologies—from the dial-in bulletin board systems of the 1970s to the World Wide Web—to access, trade, and distribute pornography, including child pornography.<sup>17</sup> Today, child pornography is available through virtually every Internet technology (see table 1).

---

<sup>15</sup>John Carr, *Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children*, NCH Children's Charities, Children & Technology Unit (Yokohama, 2001). ([http://www.ecpat.net/eng/Ecpat\\_inter/projects/monitoring/wc2/yokohama\\_theme\\_child\\_pornography.pdf](http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf))

<sup>16</sup>Susannah Fox and Oliver Lewis, *Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy*, Pew Internet & American Life Project (Apr. 2, 2001). ([http://www.pewInternet.org/reports/pdfs/PIP\\_Fear\\_of\\_crime.pdf](http://www.pewInternet.org/reports/pdfs/PIP_Fear_of_crime.pdf))

<sup>17</sup>Frederick E. Allen, "When Sex Drives Technological Innovation and Why It Has to," *American Heritage Magazine*, vol. 51, no. 5 (September 2000), p. 19. (<http://www.plannedparenthood.org/education/updatearch.html>) Allen notes that pornographers have driven the development of some of the Internet technologies, including the development of systems used to verify on-line financial transactions and that of digital watermarking technology to prevent the unauthorized use of on-line images.

---

---

**Table 1: Internet Technologies Providing Access to Child Pornography**

<b>Technology</b>	<b>Characteristics</b>
World Wide Web	Web sites provide on-line access to text and multimedia materials identified and accessed through the uniform resource locator (URL).
Usenet	A distributed electronic bulletin system, Usenet offers over 80,000 newsgroups, with many newsgroups dedicated to sharing of digital images.
Peer-to-peer file-sharing programs	Internet applications operating over peer-to-peer networks enable direct communication between users. Used largely for sharing of digital music, images, and video, peer-to-peer applications include BearShare, Gnutella, LimeWire, and KaZaA. KaZaA is the most popular, with over 3 million KaZaA users sharing files at any time.
E-mail	E-mail allows the transmission of messages over a network or the Internet. Users can send E-mail to a single recipient or broadcast it to multiple users. E-mail supports the delivery of attached files, including image files.
Instant messaging	Instant messaging is not a dial-up system like the telephone; it requires that both parties be on line at the same time. AOL's Instant Messenger and Microsoft's MSN Messenger and Internet Relay Chat are the major instant messaging services. Users may exchange files, including image files.
Chat and Internet Relay Chat	Chat technologies allow computer conferencing using the keyboard over the Internet between two or more people.

Source: GAO.

Among the principal channels for the distribution of child pornography are commercial Web sites, Usenet newsgroups, and peer-to-peer networks.<sup>18</sup>

*Web sites.* According to recent estimates, there are about 400,000 commercial pornography Web sites worldwide,<sup>19</sup> with some of the sites selling pornographic images of children. The profitability and the worldwide reach of the child pornography trade was recently demonstrated by an international child pornography ring that included a Texas-based firm providing credit card billing and password access services for one Russian and two Indonesian child pornography Web sites.

---

<sup>18</sup>According to Department of Justice officials, other forums and technologies are used to disseminate pornography on the Internet. These include Web portal communities such as Yahoo! Groups and MSN Groups, as well as file servers operating on Internet Relay Chat channels.

<sup>19</sup>Dick Thornburgh and Herbert S. Lin, editors, *Youth, Pornography, and The Internet*, National Academy Press (Washington, D.C.: 2002). ([http://www.nap.edu/html/youth\\_internet/](http://www.nap.edu/html/youth_internet/))

---

According to the U.S. Postal Inspection Service, the ring grossed as much as \$1.4 million in just 1 month selling child pornography to paying customers.

*Usenet.* Usenet newsgroups are also providing access to pornography, with several of the image-oriented newsgroups being focused on child erotica and child pornography. These newsgroups are frequently used by commercial pornographers who post “free” images to advertise adult and child pornography available for a fee from their Web sites. The increase in the availability of child pornography in Usenet newsgroups represents a change from the mid-1990’s, when a 1995–96 study of 9,800 randomly selected images taken from 32 Usenet newsgroups found that only a small fraction of posted images contained child pornography themes.<sup>20</sup>

*Peer-to-peer networks.* Although peer-to-peer file-sharing programs are largely known for the extensive sharing of copyrighted digital music,<sup>21</sup> they are emerging as a conduit for the sharing of child pornography images and videos. A recent study by congressional staff found that one use of file-sharing programs is to exchange pornographic materials, such as adult videos.<sup>22</sup> The study found that a single search for the term “porn” using a similar file-sharing program yielded over 25,000 files, more than 10,000 of which were video files appearing to contain pornographic images. In another study, focused on the availability of pornographic video files on peer-to-peer sharing networks, a sample of 507 pornographic video files retrieved with a file-sharing program included about 3.7 percent child pornography videos.<sup>23</sup>

---

<sup>20</sup>Michael D. Mehta, “Pornography in Usenet: A Study of 9,800 Randomly Selected Images,” *CyberPsychology and Behavior*, vol. 4, no. 6 (2001).

<sup>21</sup>According to the Yankee Group, a technology research and consulting firm, Internet users aged 14 and older downloaded 5.16 billion audio files in the United States via unlicensed file-sharing services in 2001.

<sup>22</sup>Minority Staff, *Children’s Access to Pornography through Internet File-Sharing Programs*, Special Investigations Division, Committee on Government Reform, U.S. House of Representatives (July 27, 2001). ([http://www.house.gov/reform/min/pdfs/pdf\\_inves/pdf\\_pornog\\_rep.pdf](http://www.house.gov/reform/min/pdfs/pdf_inves/pdf_pornog_rep.pdf))

<sup>23</sup>Michael D. Mehta, Don Best, and Nancy Poon, “Peer-to-Peer Sharing on the Internet: An Analysis of How Gnutella Networks Are Used to Distribute Pornographic Material,” *Canadian Journal of Law and Technology*, vol. 1, no. 1 (January 2002). ([http://cjlt.dal.ca/vol1\\_no1/articles/01\\_01\\_MeBePo\\_gnutella.pdf](http://cjlt.dal.ca/vol1_no1/articles/01_01_MeBePo_gnutella.pdf))

## Several Agencies Have Law Enforcement Responsibilities Regarding Child Pornography on Peer-to-Peer Networks

Table 2 shows the key national organizations and agencies that are currently involved in efforts to combat child pornography on peer-to-peer networks.

**Table 2: Organizations and Agencies Involved with Peer-to-Peer Child Pornography Efforts**

Agency	Unit	Focus
<b>Nonprofit</b>		
National Center for Missing and Exploited Children	Exploited Child Unit	Works with the Customs Service, Postal Service, and the FBI to analyze and investigate child pornography leads.
<b>Federal entities</b>		
Department of Justice	Federal Bureau of Investigation <sup>a</sup>	Proactively investigates crimes against children. Operates a national “innocent Images Initiative” to combat Internet-related sexual exploitation of children.
	Criminal Division, Child Exploitation and Obscenity Section	Is a specialized group of attorneys who, among other things, prosecute those who possess, manufacture, or distribute child pornography. Its High Tech Investigative Unit actively conducts on-line investigations to identify distributors of obscenity and child pornography.
Department of the Treasury	U.S. Customs Service CyberSmuggling Center <sup>a</sup>	Conducts international child pornography investigations as part of its mission to investigate international criminal activity conducted on or facilitated by the Internet.
	U.S. Secret Service <sup>a</sup>	Provides forensic and technical assistance in matters involving missing and sexually exploited children.

Source: GAO.

<sup>a</sup>Agency has staff assigned to NCMEC.

The National Center for Missing and Exploited Children (NCMEC), a federally funded nonprofit organization, serves as a national resource center for information related to crimes against children. Its mission is to find missing children and prevent child victimization. The center’s Exploited Child Unit operates the CyberTipline, which receives child pornography tips provided by the public; its CyberTipline II also receives tips from Internet service providers. The Exploited Child Unit investigates and processes tips to determine if the images in question constitute a violation of child pornography laws. The CyberTipline provides investigative leads to the Federal Bureau of Investigation (FBI), U.S. Customs, the Postal Inspection Service, and state and local law enforcement agencies. The FBI and the U.S. Customs also investigate leads from Internet service providers via the Exploited Child Unit’s

---

CyberTipline II. The FBI, Customs Service, Postal Inspection Service, and Secret Service have staff<sup>24</sup> assigned directly to NCMEC as analysts.

Two organizations in the Department of Justice have responsibilities regarding child pornography: the FBI and the Justice Criminal Division's Child Exploitation and Obscenity Section (CEOS).<sup>25</sup>

- The FBI investigates various crimes against children, including federal child pornography crimes involving interstate or foreign commerce. It deals with violations of child pornography laws related to the production of child pornography; selling or buying children for use in child pornography; and the transportation, shipment, or distribution of child pornography by any means, including by computer.
- CEOS prosecutes child sex offenses and trafficking in women and children for sexual exploitation. Its mission includes prosecution of individuals who possess, manufacture, produce, or distribute child pornography; use the Internet to lure children to engage in prohibited sexual conduct; or traffic in women and children interstate or internationally to engage in sexually explicit conduct.

Two organizations in the Department of the Treasury have responsibilities regarding child pornography: the Customs Service<sup>26</sup> and the Secret Service.

- The Customs Service targets illegal importation and trafficking in child pornography and is the country's front line of defense in combating child pornography distributed through various channels, including the Internet. Customs is involved in cases with international links, focusing on pornography that enters the United States from foreign countries. The Customs CyberSmuggling Center has the lead in the investigation of international and domestic criminal activities conducted on or facilitated by the Internet, including the sharing and distribution of child pornography on peer-to-peer networks. Customs maintains a reporting

---

<sup>24</sup>In commenting on our report, the Secret Service noted that its staff assigned to NCMEC include analysts and an agent.

<sup>25</sup>Two additional Justice agencies are involved in combating child pornography: the U.S. Attorneys Offices and the Office of Juvenile Justice and Delinquency Prevention. The 94 U.S. Attorneys Offices can prosecute federal child exploitation-related cases; the Office of Juvenile Justice and Delinquency Prevention funds the Internet Crimes Against Children Task Force Program, which encourages multijurisdictional and multiagency responses to crimes against children involving the Internet.

<sup>26</sup>Under the Homeland Security Act of 2002, the Customs Service is to become part of the new Department of Homeland Security.

---

link with NCMEC, and it acts on tips received via the CyberTipline from callers reporting instances of child pornography on Web sites, Usenet newsgroups, chat rooms, or the computers of users of peer-to-peer networks. The center also investigates leads from Internet service providers via the Exploited Child Unit's CyberTipline II.

- The U.S. Secret Service does not investigate child pornography cases on peer-to-peer networks; however, it does provide forensic and technical support to NCMEC, as well as to state and local agencies involved in cases of missing and exploited children.

In November 2002, we reported that federal agencies are effectively coordinating their efforts to combat child pornography, and we recommended that the Attorney General designate the Postal Inspection Service and Secret Service as agencies that should receive reports and tips of child pornography under the Protection of Children from Sexual Predators Act of 1998 in addition to the FBI and Customs.<sup>27</sup>

The Department of Justice, while agreeing with our finding that federal agencies have mechanisms in place to coordinate their efforts, did not fully support our conclusion and recommendation that federal coordination efforts would be further enhanced if the Postal Inspection Service and the Secret Service were provided direct access to tips reported to NCMEC by remote computing service and electronic communication service providers. Justice said that the FBI and Customs, the agencies that currently have direct access, can and do share these tips with the Secret Service and the Postal Inspection Service, as appropriate, and Justice believes that this coordination has been effective. Justice questioned whether coordination would be further enhanced by having the Secret Service and the Postal Inspection Service designated to receive access to these tips directly from NCMEC; however, Justice said that it is studying this issue as it finalizes regulations implementing the statute.

---

## Peer-to-Peer Applications Provide Easy Access to Child Pornography

Child pornography is easily shared and accessed through peer-to-peer file-sharing programs. Our analysis of 1,286 titles and file names identified through KaZaA searches on 12 keywords<sup>28</sup> showed that 543 (about 42 percent) of the images had titles and file names associated with child

---

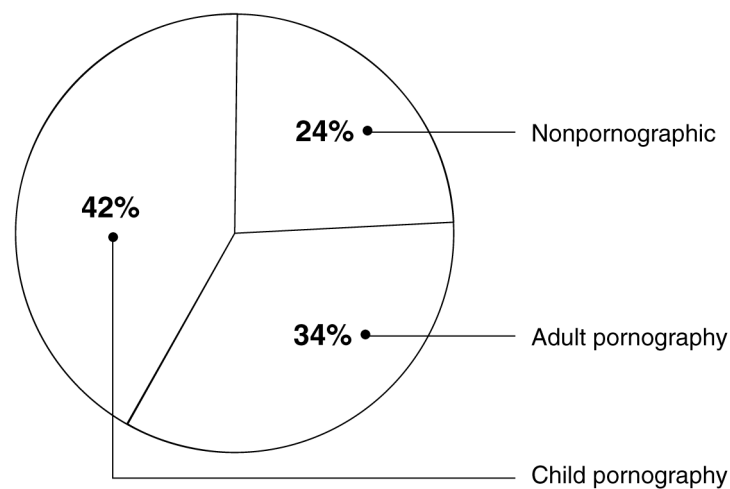
<sup>27</sup>U.S. General Accounting Office, *Combating Child Pornography: Federal Agencies Coordinate Law Enforcement Efforts, but an Opportunity Exists for Further Enhancements*, [GAO-03-272](#) (Washington, D.C.: Nov. 29, 2002).

<sup>28</sup>The 12 keywords were provided by the Cybersmuggling Center as examples known to be associated with child pornography on the Internet.

---

pornography images.<sup>29</sup> Of the remaining files, 34 percent were classified as adult pornography, and 24 percent as nonpornographic (see fig. 1). No files were downloaded for this analysis.

**Figure 1: Classification of 1,286 Titles and File Names of Images Identified in KaZaA Search**



Source: GAO.

The ease of access to child pornography files was further documented by retrieval and analysis of image files, performed on our behalf by the Customs CyberSmuggling Center. Using 3 of the 12 keywords that we used to document the availability of child pornography files, a CyberSmuggling Center analyst used KaZaA to search, identify, and download 305 files, including files containing multiple images and duplicates. The analyst was able to download 341 images from the 305 files identified through the KaZaA search.

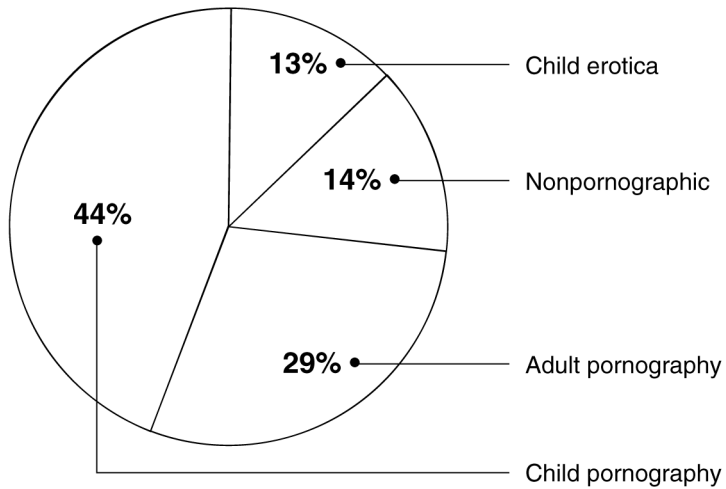
The CyberSmuggling Center analysis of the 341 downloaded images showed that 149 (about 44 percent) of the downloaded images contained child pornography (see fig. 2). The center classified the remaining images as child erotica (13 percent), adult pornography (29 percent), or nonpornographic (14 percent).

---

<sup>29</sup>We categorized a file as child pornography if one keyword indicating a minor and one word with a sexual connotation occurred in either the title or file name. Files with sexual connotation in title or name but without age indicators were classified as adult pornography.



**Figure 2: Classification of 341 Images Downloaded through KaZaA**



Source: Customs CyberSmuggling Center.

Note: GAO analysis of data provided by the Customs CyberSmuggling Center.

These results are consistent with the observations of NCMEC, which has stated that peer-to-peer technology is increasingly popular for the dissemination of child pornography. However, it is not the most prominent source for child pornography. As shown in table 3, since 1998, most of the child pornography referred by the public to the CyberTipline was found on Internet Web sites. Since 1998, the center has received over 76,000 reports of child pornography, of which 77 percent concerned Web sites, and only 1 percent concerned peer-to-peer networks. Web site referrals have grown from about 1,400 in 1998 to over 26,000 in 2002—or about a nineteenfold increase. NCMEC did not track peer-to-peer referrals until 2001. In 2002, peer-to-peer referrals increased more than fourfold, from 156 to 757, reflecting the increased popularity of file-sharing programs.

**Table 3: NCMEC CyberTipline Referrals to Law Enforcement Agencies, Fiscal Years 1998–2002**

Technology	Number of tips				
	1998	1999	2000	2001	2002
Web sites	1,393	3,830	10,629	18,052	26,759
E-mail	117	165	120	1,128	6,245
Peer-to-peer	—	—	—	156	757
Usenet newsgroups & bulletin boards	531	987	731	990	993
Unknown	90	258	260	430	612
Chat rooms	155	256	176	125	234
Instant Messaging	27	47	50	80	53
File Transfer Protocol	25	26	58	64	23
<b>Total</b>	<b>2,338</b>	<b>5,569</b>	<b>12,024</b>	<b>21,025</b>	<b>35,676</b>

Source: Exploited Child Unit, National Center for Missing and Exploited Children.

## Juvenile Users of Peer-to-Peer Applications May Be Inadvertently Exposed to Pornography

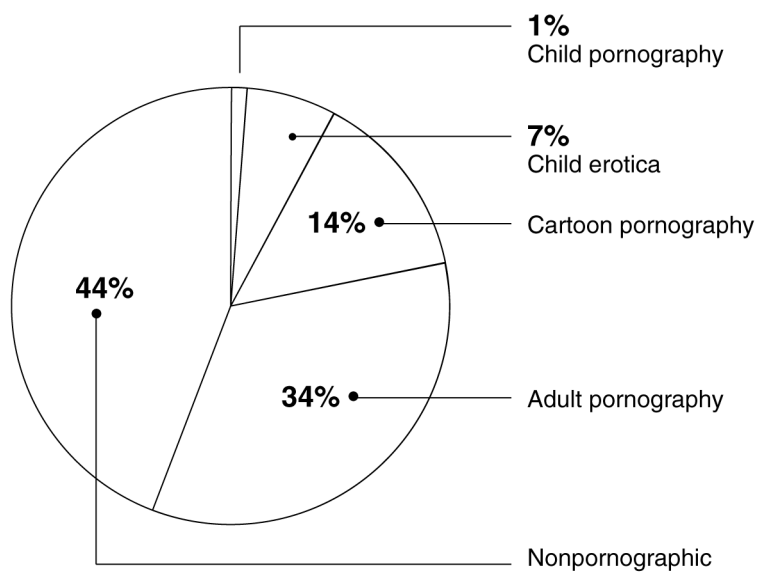
Juvenile users of peer-to-peer networks face a significant risk of inadvertent exposure to pornography when searching and downloading images. In a search using innocuous keywords likely to be used by juveniles searching peer-to-peer networks (such as names of popular singers, actors, and cartoon characters), almost half of the images downloaded were classified as adult or cartoon pornography. Juvenile users may also be inadvertently exposed to child pornography through such searches, but the risk of such exposure is smaller than that of exposure to pornography in general.

To document the risk of inadvertent exposure of juvenile users to pornography, the Customs CyberSmuggling Center performed KaZaA searches using innocuous keywords that would likely be used by juveniles. The center image searches used three keywords representing the names of a popular female singer, child actors, and a cartoon character. A center analyst performed the search, retrieval, and analysis of the images, each of which was classified into one of five categories: child pornography, child erotica, adult pornography, cartoon pornography, or nonpornographic. The searches produced 157 files, some of which were duplicates. The analyst was able to download 177 images from the 157 files identified through the search.

As shown in figure 3, our analysis of the CyberSmuggling Center’s classification of the 177 downloaded images determined that 61 images contained adult pornography (34 percent), 24 images consisted of cartoon

pornography (14 percent), 13 images contained child erotica (7 percent), and 2 images (1 percent) contained child pornography. The remaining 77 images were classified as nonpornographic.

**Figure 3: Classification of 177 Images of a Popular Singer, Child Actors, and a Cartoon Character Downloaded through KaZaA**



Source: Customs CyberSmuggling Center.

Note: GAO analysis of data provided by the Customs CyberSmuggling Center.

## Federal Law Enforcement Agencies Are Beginning to Focus Resources on Child Pornography on Peer-to-Peer Networks

Because law enforcement agencies do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet, we were unable to quantify the resources devoted to investigations concerning peer-to-peer networks. These agencies (including the FBI, CEOS, and Customs) do devote significant resources to combating child exploitation and child pornography in general. Law enforcement officials told us, however, that as tips concerning child pornography on the peer-to-peer networks increase, they are beginning to focus more law enforcement resources on this issue.

In fiscal year 2002, the key organizations involved in combating child pornography on peer-to-peer networks reported the following levels of funding:

- 
- NCMEC received about \$12 million for its congressionally mandated role as the national resource center and clearinghouse. NCMEC also received about \$10 million for law enforcement training and about \$3.3 million for the Exploited Child Unit and the promotion of its CyberTipline. From the appropriated amounts, NCMEC allocated \$916,000 to combat child pornography and referred 913 tips concerning peer-to-peer networks to law enforcement agencies.
  - The FBI allocated \$38.2 million and 228 agents and support personnel to combat child pornography through its Innocent Images unit. Since fiscal year 1996, the Innocent Image National Initiative opened 7,067 cases, obtained 1,811 indictments, performed 1,886 arrests, and secured 1,850 convictions or pretrial diversions in child pornography cases. According to FBI officials, they are aware of the use of peer-to-peer networks to disseminate child pornography and have efforts under way to work with some of the peer-to-peer companies to solicit their cooperation in dealing with this issue.
  - CEOS allocated \$4.38 million and 28 personnel to combat child exploitation and obscenity offenses. It has recently launched an effort, the High Tech Investigative Unit, dealing with investigating any Internet medium that distributes child pornography, including peer-to-peer networks.
  - Customs allocated \$15.6 million and over 144,000 hours to combating child exploitation and obscenity offenses.<sup>30</sup> The CyberSmuggling Center is beginning to actively monitor the file sharing of child pornography on peer-to-peer networks and is devoting one half-time investigator to this effort. As of December 16, 2002, the center has sent 21 peer-to-peer investigative leads to the field offices for follow-up action. Four of these leads have search warrants pending, two have been referred to local law enforcement, and five have been referred to foreign law enforcement agencies.

In addition, to facilitate the identification of the victims of child pornographers, the CyberSmuggling Center is devoting resources to the National Child Victim Identification Program, a consolidated information system containing seized images that is designed to allow law enforcement officials to quickly identify and combat the current abuse of children associated with the production of child pornography. The system's database is being populated with all known and unique child pornographic images obtained from national and international law enforcement sources

---

<sup>30</sup>Customs is unable to separate the staff hours devoted or funds obligated to combating child pornography from those dedicated to combating child exploitation in general.

---

and from CyberTipline reports filed with NCMEC. It will initially hold over 100,000 images that have been collected by federal law enforcement agencies from various sources, including old child pornography magazines.<sup>31</sup> According to Customs officials, this information will help, among other things, to determine whether actual children were used to produce child pornography images by matching them with images of children from magazines published before modern imaging technology was invented. Such evidence can be used to counter the assertion that only virtual children appear in certain images.

The system is housed at the Customs CyberSmuggling Center and is to be accessed remotely in “read only” format by the FBI, CEOS, the U.S. Postal Inspection Service, and NCMEC. An initial version of the system was deployed at the Customs CyberSmuggling Center in September 2002; the system became operational in January 2003.<sup>32</sup>

---

## Conclusions

It is easy to access and download child pornography on peer-to-peer networks. Juvenile users of peer-to-peer networks also face a significant risk of inadvertent exposure to pornography, including child pornography. We were unable to determine the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks; the key law enforcement agencies devote resources to combating child exploitation and child pornography in general, but they do not track the resources dedicated to peer-to-peer technologies in particular.

---

## Agency Comments and Our Evaluation

The Assistant Attorney General, Criminal Division, Department of Justice, provided written comments on a draft of this report, which are reprinted in appendix III. The Department of Justice agreed with the report’s findings, provided additional information on the mission and capabilities of the High Tech Investigative Unit (part of its Criminal Division’s Child Exploitation and Obscenity Section), and offered comments on the description and purpose of Customs’ National Child Victim Identification

---

<sup>31</sup>According to federal law enforcement agencies, most of the child pornography published before 1970 has been digitized and made widely available on the Internet.

<sup>32</sup>One million dollars has already been spent on the system, with an additional \$5 million needed for additional hardware, the expansion of the image database, and access for all involved agencies. The 10-year lifecycle cost of the system is estimated to be \$23 million.

---

Program. In response, we have revised our report to add these clarifications. We also received written technical comments from the Department of Justice, which we have incorporated as appropriate.

We received written technical comments from the Assistant Director, Office of Inspection, U.S. Secret Service, and from the Acting Director, Office of Planning, U.S. Customs Service. Their comments have been incorporated in the report as appropriate.

---

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Chairmen and Ranking Minority Members of other Senate and House committees and subcommittees that have jurisdiction and oversight responsibility for the Departments of Justice and the Treasury. We will also send copies to the Attorney General and to the Secretary of the Treasury. Copies will be made available to others on request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions concerning this report, please call me at (202) 512-6240 or Mirko J. Dolak, Assistant Director, at (202) 512-6362. We can be also reached by E-mail at [koontzl@gao.gov](mailto:koontzl@gao.gov) and [dolakm@gao.gov](mailto:dolakm@gao.gov), respectively. Key contributors to this report were Barbara S. Collier, James M. Lager, Neelaxi V. Lakhmani, James R. Sweetman, Jr., and Jessie Thomas.



Linda D. Koontz  
Director, Information Management Issues

---

# Appendix I: Objectives, Scope, and Methodology

---

Our objectives were to

- determine the ease of access to child pornography on peer-to-peer networks,
- assess the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography, and
- determine the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

To determine the availability of child pornography on peer-to-peer networks, we used a popular peer-to-peer application—KaZaA—to search for and identify image files that appear to be child pornography. Our analysts used keywords provided by the Customs CyberSmuggling Center. These keywords were intended to identify pornographic images; examples of the keywords include *preteen*, *underage*, and *incest*.

Once the names and titles of image files were gathered, we classified and analyzed them based on file names and keywords. Each file was classified as child pornography, adult pornography, or nonpornographic. For a file to be considered possible child pornography, the title, file name, or both had to include at least one word with a sexual connotation and an age-related keyword indicating that the subject is a minor. Files depicting adult pornography included any file that had words of a sexual nature in the title or file name. No files were downloaded for this analysis.

To determine the ease of access, we used three keywords from the initial list to perform another search. The resulting files were downloaded, saved, and analyzed by a Customs agent. Because child pornography cannot be accessed legally other than by law enforcement agencies, we relied on Customs to download and analyze files. Our own analyses were based on keywords and file names only. The Customs agent classified each of the downloaded files into one of four categories: child pornography, child erotica, adult pornography, or nonpornographic. The user with the largest number of shared files that appeared to be child pornography was also identified, and the shared folder was captured. The titles and names of files in the user's shared directory were then analyzed and classified by a GAO analyst using the same classification criteria used in original analysis.

To assess the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, a CyberSmuggling Center analyst conducted another search using three keywords that are names of popular celebrities and a cartoon character. The Customs analyst performed the search, retrieval, and analysis of the images. Each of the images downloaded was

---

classified into one of five categories: adult pornography, child pornography, child erotica, cartoon pornography, or nonpornographic.

To determine what federal law enforcement resources were allocated to combating child pornography on peer-to-peer networks, we obtained resource allocation data and interviewed officials at the U.S. Customs Service, the Department of Justice's Child Exploitation and Obscenity Section, and the Federal Bureau of Investigation. We also received information about what resources were being allocated to combat child pornography from the U.S. Secret Service and the National Center for Missing and Exploited Children.

We performed our work between July and October 2002 at the U.S. Secret Service in Baltimore, Maryland, and the U.S. Customs Service, Customs CyberSmuggling Center, in Fairfax, Virginia, under the Department of the Treasury; and at the Child Exploitation and Obscenity Section and the Federal Bureau of Investigation, under the Department of Justice, in Washington, D.C. We also worked with the National Center for Missing and Exploited Children in Alexandria, Virginia. Our work was conducted in accordance with generally accepted government auditing standards.



---

# Appendix II: Description of File Sharing and Peer-to-Peer Networks

---

Peer-to-peer file-sharing programs represent a major change in the way Internet users find and exchange information. Under the traditional Internet client/server model, the access to information and services is accomplished by the interaction between users (clients) and servers—usually Web sites or portals. A client is defined as a requester of services, and a server is defined as the provider of services. Unlike the traditional model, the peer-to-peer model enables consenting users—or peers—to directly interact and share information with each other without the intervention of a server. A common characteristic of peer-to-peer programs is that they build virtual networks with their own mechanisms for routing message traffic.<sup>1</sup>

The ability of peer-to-peer networks to provide services and connect users directly has resulted in a large number<sup>2</sup> of powerful applications built around this model.<sup>3</sup> These range from the SETI@home network (where users share the computing power of their computers to search for extraterrestrial life) to the popular KaZaA file-sharing program (used to share music and other files).

As shown in figure 4,<sup>4</sup> there are two main models of peer-to-peer networks: (1) the centralized model, based on a central server or broker that directs traffic between individual registered users, and (2) the decentralized

---

<sup>1</sup>Matei Ripenau, Ian Foster, and Adriana Iamnitchi, “Mapping the Gnutella Network: Properties of Large Scale Peer-to-Peer Systems and Implication for System Design,” *IEEE Internet Computing*, vol. 6, no. 1 (January–February 2002). ([people.cs.uchicago.edu/~matei/PAPERS/ic.pdf](http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf))

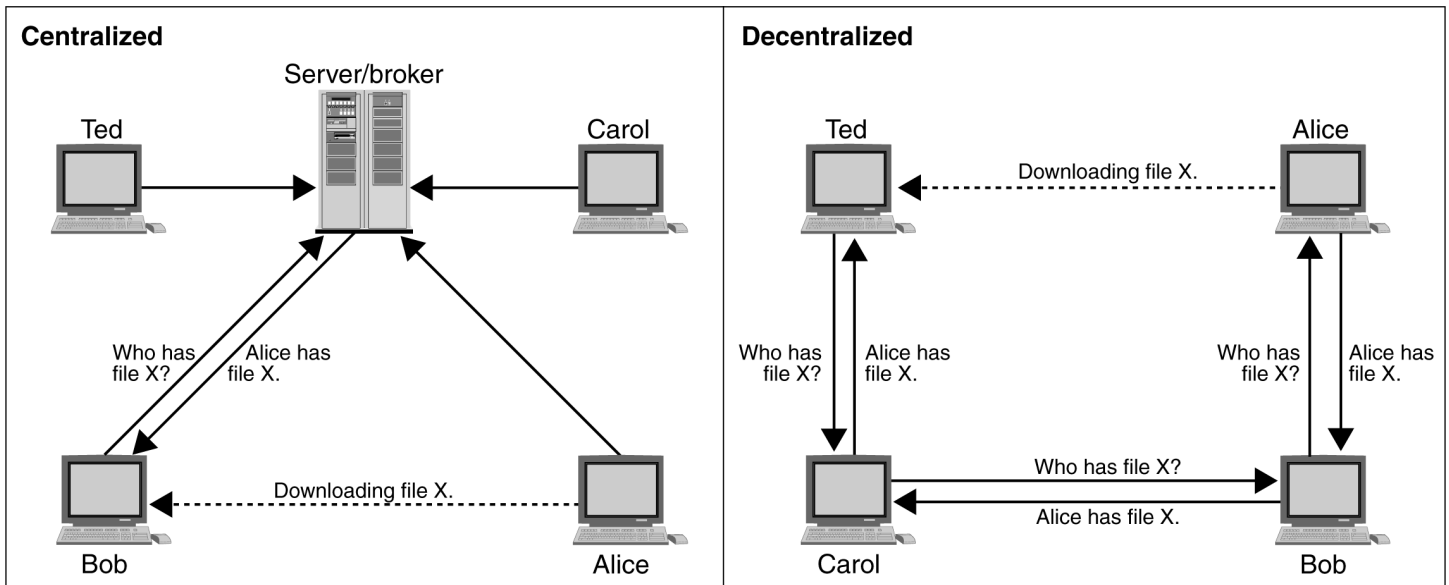
<sup>2</sup>Zeropaid.com, a file-sharing portal, lists 88 different peer-to-peer file-sharing programs available for download. (<http://www.zeropaid.com/php/filessharing.php>)

<sup>3</sup>Geoffrey Fox and Shrideep Pallickara, “Peer-to-Peer Interactions in Web Brokering Systems,” *Ubiquity*, vol. 3, no. 15 (May 28–June 3, 2002) (published by Association of Computer Machinery). ([http://www.acm.org/ubiquity/views/g\\_fox\\_2.html](http://www.acm.org/ubiquity/views/g_fox_2.html))

<sup>4</sup>Illustration adapted by Lt. Col. Mark Bontrager from original by Bob Knighten, “Peer-to-Peer Computing,” briefing to Peer-to-Peer Working Groups (August 24, 2000), in Mark D. Bontrager, *Peering into the Future: Peer-to-Peer Technology as a Model for Distributed Joint Battlespace Intelligence Dissemination and Operational Tasking*, Thesis, School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Alabama (June 2001).

model, based on the Gnutella<sup>5</sup> network, in which individuals find and interact directly with each other.

Figure 4: Peer-to-Peer Models



Source: Mark Bontrager, Bob Knighten.

Note: Adapted from Mark Bontrager's adaptation of original by Bob Knighten.

As shown in figure 4, the centralized model relies on a central server/broker to maintain directories of shared files stored on the respective computers of the registered users of the peer-to-peer network. When Bob submits a request for a particular file, the server/broker creates a list of files matching the search request by checking the request with its database of files belonging to registered users currently connected to the network. The broker then displays that list to Bob, who can then select the desired file from the list and open a direct link with Alice's computer, which currently has the file. The download of the actual file takes place directly from Alice to Bob.

<sup>5</sup>According to LimeWire LLC, the developer of a popular file-sharing program, Gnutella was originally designed by Nullsoft, a subsidiary of America Online. The development of the Gnutella protocol was halted by AOL management shortly after the protocol was made available to the public. Using downloads, programmers reverse-engineered the software and created their own Gnutella software packages. (<http://www.limewire.com/index.jsp/p2p>)

The broker model was used by Napster, the original peer-to-peer network, facilitating mass sharing of copyrighted material by combining the file names held by thousands of users into a searchable directory that enabled users to connect with each other and download MP3 encoded music files. The broker model made Napster vulnerable to legal challenges<sup>6</sup> and eventually led to its demise in September 2002.

Although Napster was litigated out of existence and its users fragmented among many alternative peer-to-peer services, most current-generation peer-to-peer networks are not dependent on the server/broker that was the central feature of the Napster service, so, according to Gartner,<sup>7</sup> these networks are less vulnerable to litigation from copyright owners.

In the decentralized model, no brokers keep track of users and their files. To share files using the decentralized model, Ted starts with a networked computer equipped with a Gnutella file-sharing program, such as KaZaA or BearShare. Ted connects to Carol, Carol to Bob, Bob to Alice, and so on. Once Ted's computer has announced that it is "alive" to the various members of the peer network, it can search the contents of the shared directories of the peer network members. The search request is sent to all members of the network, starting with Carol, who will each in turn send the request to the computers to which they are connected, and so forth. If one of the computers in the peer network (say, for example, Alice's) has a file that matches the request, it transmits the file information (name, size, type, etc.) back through all the computers in the pathway towards Ted, where a list of files matching the search request appears on Ted's computer through the file-sharing program. Ted will then be able to open a connection with Alice and download the file directly from Alice's computer.<sup>8</sup>

One of the key features of Napster and the current generation of decentralized peer-to-peer technologies is their use of a virtual name space (VNS). A VNS dynamically associates user-created names with the Internet address of whatever Internet-connected computer users happen to be

---

<sup>6</sup>*A&M Records v. Napster*, 114 F.Supp.2d 896 (N.D. Cal. 2000).

<sup>7</sup>Lydia Leong, "RIAA vs. Verizon, Implications for ISPs," Gartner (Oct. 24, 2002).

<sup>8</sup>LimeWire, *Modern Peer-to-Peer File Sharing over the Internet*.  
(<http://www.limewire.com/index.jsp/p2p>)

using when they log on.<sup>9</sup> The VNS facilitates point-to-point interaction between individuals, because it removes the need for users and their computers to know the addresses and locations of other users; the VNS can, to certain extent, preserve users' anonymity and provide information on whether a user is or is not connected to the Internet at a given moment.<sup>10</sup>

The file-sharing networks that result from the use of peer-to-peer technology are both extensive and complex. Figure 5 shows a map or topology of a Gnutella network whose connections were mapped by a network visualization tool.<sup>11</sup> The map, created in December 2000, shows 1,026 nodes (computers connected to more than one computer) and 3,752 edges (computers on the edge of the network connected to a single computer). This map is a snapshot showing a network in existence at a given moment; these networks change constantly as users join and depart them.

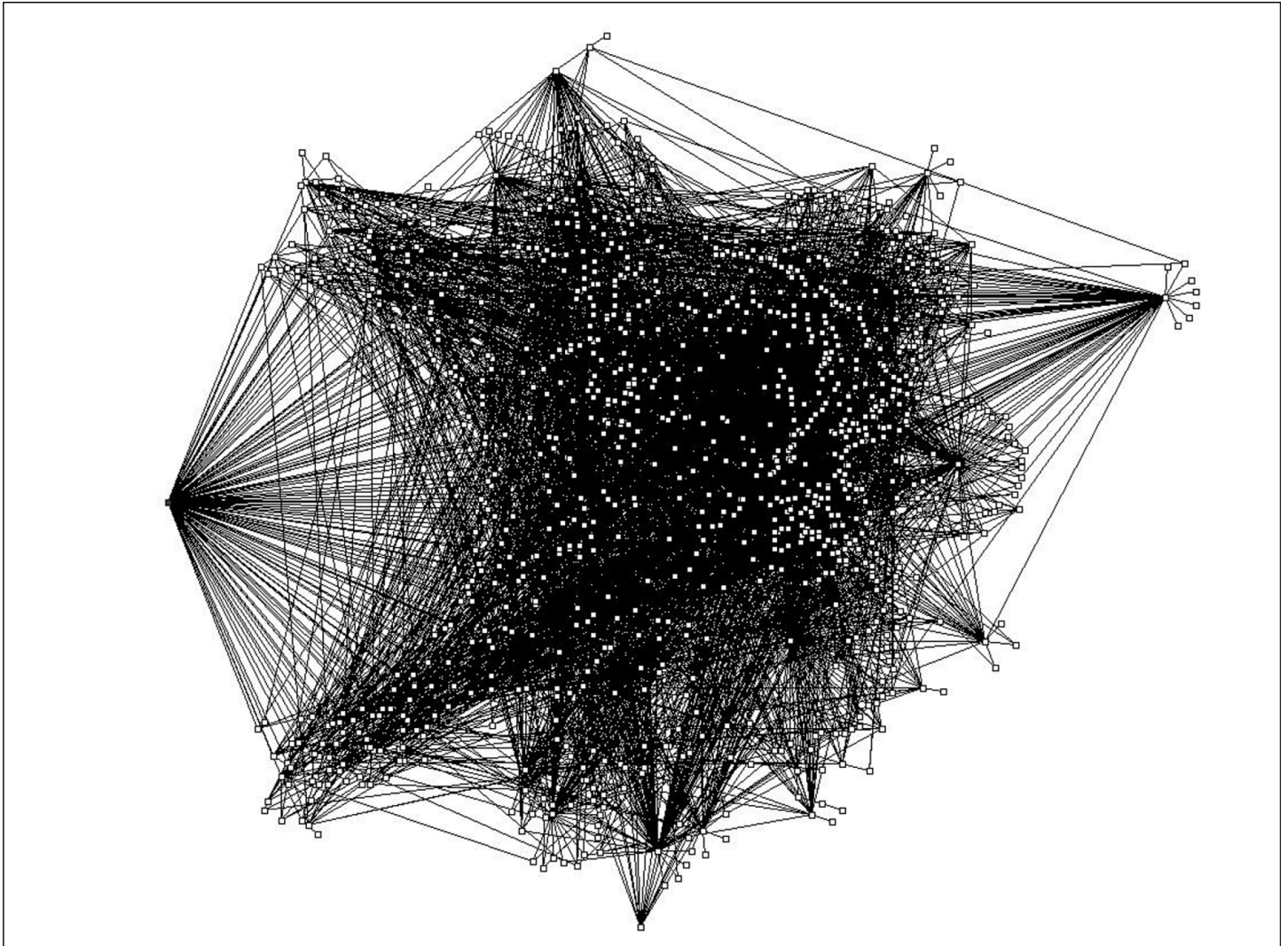
---

<sup>9</sup>S. Hayward and R. Batchelder, "Peer-to-Peer: Something Old, Something New," Gartner (Apr. 10, 2001).

<sup>10</sup>Peer-to-peer users may appear to be but are not anonymous. Law enforcement agents may identify users' Internet addresses during the file-sharing process and obtain, under a court order, their identities from their Internet service providers.

<sup>11</sup>Mihajlo A. Jovanovic, Fred S. Annexstein, and Kenneth A. Berman, *Scalability Issues in Large Peer-to-Peer Networks: A Case Study of Gnutella*, University of Cincinnati Technical Report (2001). (<http://www.ececs.uc.edu/~mjovanov/Research/paper.html>)

Figure 5: Topology of a Gnutella Network



Source: Mihajlo A. Jovanovic, Fred S. Annexstein, and Kenneth A. Berman, Laboratory of Networks and Applied Graph Theory, University of Cincinnati.

# Appendix III: Comments from the Department of Justice



U.S. Department of Justice

Criminal Division

*Office of the Assistant Attorney General*

*Washington, D.C. 20530*

February 3, 2003

Ms. Linda D. Koontz  
Director  
Information Management Issues  
U.S. General Accounting Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Koontz:

The Department of Justice has reviewed the GAO proposed report entitled, "File Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography" (GAO-03-351) (the "Proposed Report"). We agree with the Proposed Report's findings that child pornography is readily available on peer-to-peer networks, that juveniles using such networks may be inadvertently exposed to child pornography as well as other pornographic material, and that federal law enforcement agencies are devoting substantial resources to fighting child exploitation and child pornography. We also would like to express our appreciation to GAO for its effort in conducting a careful, thorough, and diligent study of this important issue, and for its recognition that the Criminal Division's Child Exploitation and Obscenity Section ("CEOS") has taken an important role in combating child exploitation and child pornography.

While we support the Proposed Report's findings, we offer, as important additional context, the information set forth below describing the Department's innovative approach to meeting and anticipating the latest technology challenges and explaining, in greater detail, the full scope of the National Child Victim Identification Program.

Understanding that child pornographers are increasingly mastering and using cutting-edge technology to commit their crimes and avoid apprehension, and understanding the existence of a technology gap between law enforcement generally and the offenders, CEOS created a High Tech Investigative Unit (HTIU) within CEOS, staffed with computer forensic experts, to keep pace with misused technology and to fill that gap. The goal of the HTIU is to ensure that

Internet-based child pornography and adult obscenity prosecutions benefit from the special expertise brought to bear by technology experts. HTIU's computer forensic specialists can and do meet the challenge presented by the use of peer-to-peer networks in the commission of child pornography and adult obscenity crimes. More importantly, the Unit is poised to meet new technological challenges that will surely develop as technology evolves.

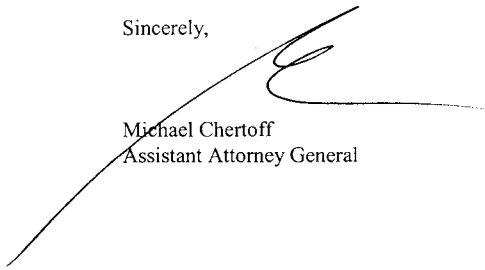
The National Child Victim Identification Program (NCVIP), discussed in the Proposed Report, exemplifies the cooperative mind-set that exists in the law enforcement community in addressing child pornography and child abuse crimes effectively and decisively. The NCVIP also exemplifies the cooperative mind-set that exists between the law enforcement community and private organizations to marshal every resource, public or private, to eradicate the trade in child pornography, identify current abuse, and bring the perpetrators to justice.

The Proposed Report characterizes the NCVIP as an "information system and database of child pornography images" intended to "help determine whether actual children were used to produce child pornography images by matching them with images of children from magazines published before modern imaging technology was invented." Proposed Report, at 16. While this description exemplifies one part of the NCVIP's design, it does not adequately explain that the NCVIP is primarily intended to help law enforcement identify and stop *current* instances of child abuse associated with the production of child pornography. The NCVIP will help stop *current* child abuse by allowing law enforcement, upon discovering an image of child pornography, quickly to determine whether that image is new or dated. If the image is new, law enforcement can then take steps to identify the victim and the producer with the goal of preventing continued abuse of the victim. For far too long, law enforcement's focus has been on the image itself – with little consideration for the serious abuse depicted in the images. The lack of focus on the abuse represented in the images stemmed mostly from the fact that investigators had no means of determining whether the abuse depicted was recent or current, or many years old. NCVIP will be instrumental in focusing law enforcement's efforts on current abuse and ensuring that our focus is not simply limited to the trafficking of child pornographic images, but extends to the investigation and prosecution of the underlying abuse. Accordingly, we recommend that the proposed report describe the NCVIP as primarily "a consolidated information system containing seized images of child pornography designed to allow law enforcement quickly to identify and combat the current abuse of children associated with the production of child pornography."

In sum, we agree that those who engage in the production and trafficking of child pornography are consistently early adopters of emerging technologies. The Department has risen to, and met, that challenge by ensuring an equal or greater level of technological expertise on the part of its prosecutors and agents investigating Internet-based child pornography and adult obscenity crimes.

I hope you will consider our comments in preparing the final GAO report on this subject. If you have any questions regarding the Department's comments, you may contact Vickie L. Sloan, Director, Audit Liaison Office, on (202) 514-0469.

Sincerely,



Michael Chertoff  
Assistant Attorney General



---

# Glossary

---

Broadband	Operating at bandwidths markedly greater than that provided by telephone networks. Broadband networks can carry digital videos or a massive quantity of data simultaneously. In the on-line environment, the term is often used to refer to Internet connections provided through cable or DSL (digital subscriber line) modems.
BearShare	A file-sharing program for Gnutella networks. BearShare supports the trading of text, images, audio, video, and software files with any other user of the network.
Broker	In the peer-to-peer environment, an intermediary computer that coordinates and manages requests between client computers.
Cartoon pornography	Images of cartoon characters engaged in sexual activity.
Chat	Internet program enabling users to communicate through short written messages. Some of the most popular chat programs are America Online's Instant Messenger and the Microsoft Network Messenger. See instant messaging.
Child erotica	Sexually arousing images of children that are not considered pornographic, obscene, or offensive.
Client-server	A networking model in which a collection of nodes (client computers) request and obtain services from a server node (server computer).
Gnutella	A file-sharing program based on the Gnutella protocol. Gnutella enables users to directly share files with one another. Unlike Napster, Gnutella-based programs do not rely on a central server to find files.
Gnutella protocol	Decentralized group membership and search protocol, typically used for file sharing. Gnutella file-sharing programs build a virtual network of participating users.

---

Hypertext language (HTML)	The standard language (HyperText Markup Language) used to display information on the Web. It uses tags embedded in text files to encode instructions for formatting and displaying the information.
Instant messaging (IM)	A popular method of Internet communication that allows for an instantaneous transmission of messages to other users who are logged into the same instant messaging service. America Online's Instant Messenger and the Microsoft Network Messenger are among the most popular instant messaging programs (see chat).
Internet relay chat (IRC)	Internet chat application allowing real-time conversations to take place via software, text commands, and channels. Unlike the Web-based IM, IRC requires special software and knowledge of technical commands (see chat).
IP address	Internet Protocol address. A number that uniquely identifies a computer connected to the Internet to other computers.
KaZaA	A file-sharing program using a proprietary peer-to-peer protocol to share files among users on the network. Through a distributed self-organizing network, KaZaA requires no broker or central server like Napster.
LimeWire	A file-sharing program running on Gnutella networks. It is open standard software running on an open protocol, free for the public to use.
Morpheus	A file-sharing application using the KaZaA peer-to-peer protocol to share files among users on the network.
Morphing	A process whereby one image is gradually transformed into a second image.
MP3	Moving Pictures Experts Group (MPEG) MPEG-1 Audio Layer-3. A widely used standard for compressing and transmitting music in digital format across Internet. MP3 can compress file sizes at a ratio of about 10:1 while preserving sound quality.

---

Newsgroups	Discussion groups on Usenet, varying in topic from technical to bizarre. There are over 80,000 newsgroups organized by major areas or domains. The major domains are alt (any conceivable topic, including pornography); biz (business products and services); rec (games and hobbies); comp (computer hardware and software); sci (sciences); humanities (art and literature); soc (culture and social issues); misc (miscellaneous, including employment and health); and talk (debates on current issues). See Usenet.
Node	A computer or a device that is connected to a network. Every node has a unique network address.
Peer	A network node that may function as a client or a server. In the peer-to-peer environment, peer computers are also called servents, since they perform tasks associated with both servers and clients.
Server	A computer that interconnects client computers, providing them with services and information; a component of the client-server model. A Web server is one type of server.
<a href="#">SETI@home</a>	Search for extraterrestrial intelligence at home. A distributed computing project, SETI@home uses data collected by the Arecibo Telescope in Puerto Rico. The project takes advantage of the unused computing capacity of personal computers. As of February 2000, the project encompassed 1.6 million participants in 224 countries.
Topology	The general structure—or map—of a network. It shows the computers and the links between them.
Usenet	A bulletin board system accessible through the Internet containing more than 80,000 newsgroups. Originally implemented in 1979, it is now probably the largest decentralized information utility in existence (see newsgroups).
Virtual	Having the properties of x while not being x. For example, “virtual reality” is an artificial or simulated environment that appears to be real to the casual observer.

---

**Virtual name space (VNS)** Internet addressing and naming system. In the peer-to-peer environment, VNS dynamically associates names created by users with the IP addresses assigned by their Internet services providers to their computers.

---

**World Wide Web** A worldwide client-server system for searching and retrieving information across the Internet. Also known as WWW or the Web.

---

## GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site ([www.gao.gov](http://www.gao.gov)) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to GAO Mailing Lists" under "Order GAO Products" heading.

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office  
441 G Street NW, Room LM  
Washington, D.C. 20548

To order by Phone:   Voice: (202) 512-6000  
                              TDD: (202) 512-2537  
                              Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:  
Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)  
E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)  
Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Public Affairs

Jeff Nelligan, Managing Director, [NelliganJ@gao.gov](mailto:NelliganJ@gao.gov) (202) 512-4800  
U.S. General Accounting Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548